

Caio dos Santos Gomes

Eduardo Sturm

Eduardo Stradiotto

João Pedro Holanda (24026658)

BANCO DE DADOS

1. Descentralização e Servidores

- O Telegram usa uma arquitetura de servidores descentralizados distribuídos em diferentes partes do mundo. Isso ajuda a melhorar a performance e a segurança, permitindo que dados de usuários sejam processados e armazenados em locais próximos a eles.
- Esses servidores são segmentados por região para oferecer uma baixa latência e um acesso mais rápido. A descentralização também permite que o Telegram opere em países onde a regulamentação pode ser rígida para armazenar dados apenas localmente.

2. Segurança e Criptografia

- O Telegram oferece criptografia de ponta a ponta para conversas secretas (chats secretos), onde apenas os dispositivos de origem e destino conseguem decifrar as mensagens.
- Para conversas normais, as mensagens são criptografadas entre o dispositivo do usuário e os servidores do Telegram, usando uma combinação de AES simétrico, RSA e o protocolo Diffie-Hellman.
- No caso dos chats secretos, as mensagens não são armazenadas nos servidores do Telegram. Já em chats comuns, elas ficam armazenadas de forma criptografada nos servidores do Telegram para possibilitar sincronização entre dispositivos.

3. Armazenamento de Dados e Sincronização

- Para chats não secretos, o Telegram armazena todas as mensagens, arquivos e mídia nos servidores. Isso permite que os usuários possam acessar seus dados de qualquer dispositivo onde o Telegram esteja instalado, sem depender de backups locais.
- O banco de dados armazena as mensagens e as mídias (imagens, vídeos, documentos), bem como outros dados, como contatos, histórico de chamadas, configurações de grupos e canais, preferências do usuário, etc.

- Quando o usuário faz login em um novo dispositivo, o aplicativo sincroniza esses dados com o servidor.

4. Controle de Cache e Armazenamento Local

- O Telegram utiliza o cache local para armazenar temporariamente os dados, como mídias e conversas recentes, no dispositivo do usuário. Isso permite uma experiência de uso mais rápida e reduz o consumo de dados.
- O usuário tem a opção de limpar o cache local, o que remove o conteúdo do dispositivo sem apagá-lo dos servidores, preservando o histórico completo de mensagens e mídias.

5. Escalabilidade e Redundância

- O Telegram lida com milhões de mensagens por segundo e usa uma estrutura de banco de dados altamente escalável. Ele faz uso de várias tecnologias, como servidores de alta capacidade e técnicas de balanceamento de carga, para garantir um serviço confiável.
- Os dados são distribuídos e replicados em diferentes servidores e regiões, garantindo que, mesmo se um servidor ou datacenter falhar, os dados do usuário permaneçam seguros e acessíveis.

6. Proteção de Dados e Privacidade

- O Telegram permite que os usuários controlem seus dados, com opções como o auto-apagamento de mensagens em chats secretos, o apagamento de histórico, e até a exclusão completa de sua conta.
- As políticas de privacidade do Telegram visam proteger os dados dos usuários e evitar qualquer forma de compartilhamento de informações com terceiros, o que é parte do compromisso de privacidade da empresa.

Esses elementos tornam o banco de dados do Telegram robusto, seguro e rápido, oferecendo aos usuários uma experiência de mensagens que prioriza tanto o desempenho quanto a segurança dos dados.